REMARKS

Claims 1-20 remain pending in the application. Applicants respectfully request reconsideration of all pending claims in light of the remarks and amendments presented herein.

Objections

The Office Action objected to the specification for failing to provide antecedent basis for the term "name" recited in claim 17. Applicant has amended claim 17 to remove the term "name".

The Office Action objected to claims 15 and 16 as being duplicate claims. Claim 16 has been amended and is now directed toward other allowable subject matter.

Claim Rejections - 35 U.S.C. §112

Claim 17 was rejected under 35 U.S.C § 112 first and second paragraphs for reciting the term "name". Applicants have amended claim 17 to remove the term "name".

Claim 19 was rejected under 35 U.S.C § 112 second paragraph for reciting "a business network link". The Office Action avers that since the term "a business network link" is not defined, the claim is rendered indefinite. To advance prosecution of the application, Applicants have amended the claim to recite "a business network" and submit that the newly recited claim language is understood by a person skilled in the art.

Claim Rejections - 35 U.S.C. §102

Claims 1, 2, 9-13, 15-16 and 19-20 were rejected under 35 U.S.C. § 102(b), as being anticipated by U.S. Patent No. 6,205,480 to Broadhurst.

Applicants' invention is directed to a system for ubiquitous network presence and access without cookies. (Application, Title). In contrast, Broadhurst's purported invention requires the use of a cookie.

Specifically, Broadhurst discloses an authentication system for accessing back end

computer applications through a computer server. (Broadhurst, Column 1, Lines 5-8). Broadhurst's authentication information is mapped to the role of a user such as "executive", "clerk" or "accounting". (Broadhurst, Column 3, Lines 19-24). The user's role determines which applications and hence which network resources can be accessed by the user. (Broadhurst, Column 3, Lines 28-31). The authentication information is mapped into a network credential which includes the role of the user. (Broadhurst, Column 3, Lines 42-44). The network credential is then formed into a cookie and the cookie sent to the browser. (Broadhurst, Figure 2, Step 108 Column 3, Line 45). The cookie containing the network credential and the role of the user allows the user to freely access any of the applications allowed for someone having the role of the user. (Broadhurst, Column 3, Line 46-48).

Applicants note that the Examiner believes that Step 104 of Broadhurst teaches *that if it is determined that if there is not yet a user cookie containing a network credential, a cookie is created* and that this teaching anticipates *matching a unique identification (ID) stored on the client to that stored either on the first or other servers when the user correspondingly communicates with either the first or other servers.* (Office Action, Page 15, Third Paragraph). Admittedly, Applicants are unable to follow the Examiner's logic and conclusion. That is, that checking for a cookie with a network credential is the same or equivalent to matching IDs stored on a client and a server.

Nevertheless, Applicants have amended claims 1, 2, 9 and 10 to recite additional features of the invention and advance prosecution of the application. For example, each of the pending claims now recites "communicating the unique customer identification to, a client running the client application, and other servers running a plurality of server applications; wherein the communication does not include a cookie sent to a browser".

As explained above, Broadhurst's authentication information and user role are packaged in a cookie and sent to a browser. (Broadhurst, Figure 2, Step 108 Column 3, Lines 42-45). This can be seen clearly in every one of Broadhurst's figures. Figure 1 shows a browser 14 on each workstation 10, with each of the browsers 14 in communication with one of the web servers 12 resident on a plurality of host machines 13. The flow chart of Figure 2 shows that if the user

does not have a cookie 104, a cookie is formed 106 and then sent to the browser 108. (Broadhurst, Figure 1 and 2). Clearly, a cookie is needed to access Broadhurst's network and is central to Broadhurst's purported invention that allows access to a network via validation of the cookie 112. (Broadhurst, Figure 2).

Broadhurst thus fails to disclose or suggest the recited feature making the claims patentable over Broadhurst. Accordingly, Applicants respectfully request that this rejection be withdrawn.

Claim Rejections - 35 U.S.C. §103

Claims 3 and 6 were rejected under 35 U.S.C. § 103(a), as being unpatentable over Broadhurst in view of U.S. Patent No. 6,324,648 to Grantges. Applicant respectfully traverses.

Grantges discloses a computer system for authenticating a user 18 through the use of a client side digital certificate. (Application, Abstract, Column 3, Line 66 – Column 4, Line 4). The digital certificate is sent to a proxy server 34 that checks the certificate to see whether the certificate has been issued by a preapproved certificate authority. (Application, Column 4, Lines 43-48). The proxy server then sends the certificate to a gateway 38 to be authenticated at a more substantive level. (Application, Column 4, Lines 48-55).

Saliently, Grantges fails to disclose or suggest "communicating the unique customer identification to, a client running the client application, and other servers running a plurality of server applications; wherein the communication does not include a cookie sent to a browser" making claims 3 and 6 patentable over Broadhurst in view of Grantjes.

Claims 5 and 8 were rejected under 35 U.S.C. § 103(a), as being unpatentable over Broadhurst in view of U.S. Patent No. 5,764,915 to Heimsoth. Applicant respectfully traverses.

Heimsoth discloses an object oriented protocol interface for establishing a communication path between communication endpoints in a computer network. (Heimsoth, Column 2, Lines 41-43). Notably, Heimsoth disclosure is not concerned with a ubiquitous network presence without cookies.

Claims 5 and 8 depend from claim 1 and are patentable for the same reasons as claim 1. Heimseth like Broadhurst is silent regarding "communicating the unique customer identification to, a client running the client application, and other servers running a plurality of server applications; wherein the communication does not include a cookie sent to a browser" making claims 5 and 8 patentable over Broadhurst in view of Heimseth.

Claims 4 and 7 were rejected under 35 U.S.C. § 103(a), as being unpatentable over Broadhurst in view of U.S. Publication No. 2002/0010776 to Lerner. Applicant respectfully traverses.

Lerner's publication is directed towards an integrated distributed shared services architecture. (Lerner, Paragraph 26). Lerner uses a cookie based architecture to provide this service. (Lerner, Paragraph 33). Browser cookies are passed over the internet from one application to another through browser redirects. (Lerner Paragraph 37). Lerner purports that this allows small amounts of user information to be passed from one server to another in authentication process. (Lerner, Paragraph 37).

Claims 4 and 7 depend from claim 1 and are patentable for the same reasons as claim 1. Lerner like Broadhurst fails to disclose "communicating the unique customer identification to, a client running the client application, and other servers running a plurality of server applications; wherein the communication does not include a cookie sent to a browser" making claims 4 and 7 patentable over Broadhurst in view of Lerner.

Claims 14 and 17 were rejected under 35 U.S.C. § 103(a), as being unpatentable over Broadhurst in view of U.S. Publication No. 2002/001 to Lerner. Applicant respectfully traverses.

Exemplary Support for the Claim Amendments

Support for the claim amendments may be found throughout the specification including the originally filed claim set. Exemplary support for the claim amendments is also provided below.

1. A method for computer network access comprising the steps of: running a client application wherein, the client application is not a web browser, (Application, Title, Page 4,

Lines 21 and 22) and the client application runs on a customer device (Application Page 4, Lines 19-20); entering user information into the customer device (Application Page 4, Line 29); communicating the entered user information to a first server; storing the user information on the first server; creating a unique customer identification for a user of the customer device (Application Page 5, Lines 11-13); storing the unique customer identification on the first server; communicating the unique customer identification to, a client running the client application, and other servers running a plurality of server applications (Application, Page 5, Liens 19-24); wherein the communication does not include a cookie sent to a browser (Application, Title, Page 5, Lines 15-16, 19-24) storing the unique customer identification on the client and the other servers; communicating the unique customer identification from the client to the first server or one of the other servers (Application, Page 5, Lines 19-24); and authenticating the user by matching the unique customer received at the first server or one of the other servers with the unique customer identification stored on the first server or one of the other servers (Application, Page 5, Line 27, Page 6, Line 1).

9. A digital computer system programmed to perform the following steps: run a client application wherein, the client application is not a web browser, (Application, Title, Page 4, Lines 21 and 22) and the client application runs on a customer device (Application Page 4, Lines 19-20); receive user information entered into the customer device (Application Page 4, Line 29); communicate the entered user information to a first server; store the user information on the first server; create a unique customer identification for a user of the customer device; store the unique customer identification on the first server; communicate the unique customer identification to, a client running the client application, and other servers running a plurality of server applications wherein the communication does not include a cookie sent to a browser; (Application, Title, Page 5, Lines 15-16, 19-24) store the unique customer identification on the client and the other servers; communicate the unique customer identification from the client to the first server or one of the other servers (Application, Page 5, Lines 19-24); and authenticate, the user by matching the unique customer identification received at the first server or one of the other servers with the unique customer identification stored on the first server or one of the other servers (Application,

Page 5, Line 27, Page 6, Line 1) wherein each of the other servers has a particular service available to the user of the customer device and wherein the user of the customer device is not allowed access to the services the unique customer identification received at the first server or one of the other servers does not match the unique customer identification stored on the first server or one of the other servers (Application, Page 5, Line 27, Page 6, Line 12).

10. (Currently Amended) A computer-readable medium storing a computer program, the computer program functional to perform the following steps: run a client application wherein, the client application is not a web browser, (Application, Title, Page 4, Lines 21 and 22) and the client application runs on a customer device (Application Page 4, Lines 19-20); receive user information entered into the customer device; communicate the entered user information to a first server; store the user information on the first server; create a unique customer identification for a user of the customer device; store the unique customer identification on the first server; communicate the unique customer identification to, a client running the client application, and other servers running a plurality of server applications; store the unique customer identification on the client and the other servers (Application, Title, Page 5, Lines 15-16, 19-24); communicate the unique customer identification from the client to the first server or one of the other servers (Application, Title, Page 5, Lines 15-16, 19-24) wherein the communication does not include a cookie sent to a browser; (Application, Title, Page 5, Lines 15-16, 19-24); and authenticate, the user by matching the unique customer identification received at the first server or one of the other servers with the unique customer identification stored on the first server or one of the other servers wherein each of the other servers has a particular service available to the user of the customer device and wherein the user of the customer device is not allowed access to the services the unique customer identification received at the first server or one of the other servers does not match the unique customer identification stored on the first server or one of the other servers (Application, Page 5, Line 27, Page 6, Line 12).

11. (Currently Amended) A computer network system comprising: a server computer running a server software application operable to; create a unique customer identification for a user, store the unique identification on the server computer, communicate the unique customer

identification to a client, and authenticate the user via the unique identification when the user communicates with the server computer; and a client computer running a client software application said client computer operably connected to the server computer over a network and wherein the client software application is operable to: communicate user information to the server application, store the unique customer indentification, and provide the server with the unique customer indentification to authenticate a user with the server application.

CONCLUSION

Applicants submit that all the pending claims are now in condition for allowance and accordingly a notice of allowance is respectfully requested.

Respectfully submitted,

Dated: 6-17-2008

Joe C. Liu
Reg. No. 61,106

Address all correspondence to:
FITCH, EVEN, TABIN & FLANNERY
120 So. LaSalle Street, Ste. 1600
Chicago, IL 60603

Direct telephone inquiries to:
Thomas F. Lebens
120 So. LaSalle Street, Ste. 1600
Chicago, IL 60603
(805) 781-2865